IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

IN RE: BPS DIRECT, LLC and CABELA'S, LLC, WIRETAPPING	**MDL NO. 3074** **2:23-md-03074-MAK**

DEFENDANTS' SUPPLEMENTAL MEMORANDUM IN RESPONSE TO ECF NO. 71

Pursuant to the Court's October 26, 2023 Order (ECF No. 71), Defendants BPS Direct, LLC and Cabela's, LLC submit the following Supplemental Memorandum addressing the questions directed at Defendants in the Court's Order—questions 1, 4, 5, 6, and 7. Additionally, per the Court's Order, Defendants advise that both lead counsel for Defendants, Jennifer McLoone who participated in the Court's prior session of oral argument, and local counsel for Defendants, Erin Leffler, will be in trial on November 14 and November 15 and may be unable to participate in a virtual oral argument on those days, depending on the time and trial activity. *See* Ex. A (Erin pLeffler - Notice of trial attachment for 15 days beginning November 2, 2023); Ex. B (Jennifer McLoone – notice from court confirming inclusion on weeks 3 and 4 (November 6-17, 2023) of trial docket). Additional counsel for Defendants can be available on either November 14 or November 15 if the Court wishes to hold further virtual oral argument and will excuse the attendance of local and lead counsel.

Question 1 – Whether Website Users sufficiently alleged facts to establish Defendants accessed Website Users' computers without authority under 18 U.S.C. § 1030(a) with their best supporting authority:

Whether Defendants accessed Website Users' computers without authority depends on whether Defendants' actions were "analogous to breaking and entering." *hiQ Labs, Inc. v. LinkedIn Corp*., 31 F.4th 1180, 1197 (9th Cir. 2022) (internal citations and quotations omitted); *see also Andrews v. Sirius XM Radio Inc*., 932 F.3d 1253, 1263 (9th Cir. 2019) (CFAA limited "to harms caused by computer intrusions[.]").

The Website Users do not (and cannot) allege that the Defendants were "breaking and entering" into their computers. Rather, the Complaint alleges that they were unlawfully recorded "[w]hile visiting Defendants' websites." Compl. ¶ 137. Moreover, Plaintiffs allege that the recording was done through "Session Replay Code embedded on [Defendants'] website[s]," not through any piece of code or other recording mechanism on Plaintiffs' devices. These allegations are not analogous to "breaking and entering" by the Defendants. To the contrary, rather than alleging a situation analogous to Defendants breaking and entering into the Website Users' homes—the Website Users have alleged that they entered the *Defendants'* house and, once inside, were recorded.

Further, the Complaint asserts that the Defendants "exceeded authorized access" to Website Users' computers, *id*. ¶ 188, but this argument is squarely foreclosed by *Van Buren v. United States*, 141 S.Ct. 1648 (2021). The Supreme Court explained in *Van Buren* that § 1030(a)(2) does "not cover those who ... have improper motives for obtaining information that is otherwise available to them." *Id*. at 1652. The Website Users do not, and cannot, allege that their activity *on Defendants' websites* was unavailable to the Defendants. Thus, Defendants cannot have "exceed[ed] authorized access" to the Website Users' computers.

Question 4 – As to the wiretap claims under the federal and Missouri laws, provide your best authority as to how we should consider applying the "criminal or tortious purpose" exception:

Multiple circuits have interpreted the "criminal or tortious purpose" exception of the Federal Wiretap Act, 18 U.S.C. § 2511(2)(d), to require a criminal or tortious intent "independent of the act of recording itself." *Caro v. Weintraub*, 618 F.3d 94, 100 (2d Cir. 2010); *see also Desnick v. American Broadcasting Cos*., 44 F.3d 1345, 1347–48 (7th Cir.1995); *Sussman v. American Broadcasting Cos*., 186 F.3d 1200, 1201 (9th Cir.1999); *Lucas v. Fox News Network, LLC*, 248 F.3d 1180, 2001 WL 100181, at *4 (11th Cir. Jan.16, 2001) (per curiam). If a complaint alleges that the underlying purpose of intercepting communications is to make money—without a "specific contemporary intention to commit a crime or tort"—then courts have concluded that the "criminal or tortious purpose" exception does not apply. *In re DoubleClick Inc. Priv. Litig*., 154 F. Supp. 2d 497, 515, 519 (S.D.N.Y. 2001); *see also In re Google Inc. Gmail Litig.*, 2014 WL 1102660, at *18 n.13 (N.D. Cal. Mar. 18, 2014); *Rodriguez v. Google LLC*, No. 20-CV-04688-RS, 2021 WL 2026726, at *6 n.8 (N.D. Cal. May 21, 2021); *Katz-Lacabe v. Oracle Am., Inc*., 2023 WL 2838118, at *10 (N.D. Cal. Apr. 6, 2023). Similarly, if a complaint alleges merely that the defendant's conduct "amounted to a tort," without any allegation that the defendant's "primary purpose was to commit a tort," courts have concluded that the exception does not apply. *Cohen v. Casper Sleep Inc*., 2018 WL 3392877, at *4 (S.D.N.Y. July 12, 2018).

Here, Plaintiffs allege that Defendants collected session replay data to make money, *see* Compl. ¶¶ 294, 337, and all the counts in the complaint stem from the collection of session replay data. Because there is no allegation of a criminal or tortious intent "independent of the act of recording itself," *Caro*, 618 F.3d at 100, the "criminal or tortious purpose" exception does not apply.

Question 5 – As to the wiretap claims under the Maryland and Massachusetts laws, describe whether and to what extent our analysis differs given the definitions of "contents" under each State's law:

The Court's analysis need not be impacted by the slightly different definition of "contents" under the Maryland and Massachusetts Wiretap Acts. Under both Acts, "contents" is defined as "information concerning identity of the parties to such communication or the existence, contents, substance, purport, or meaning of that communication." Mass. Gen. Laws ch. § 272; Md. Code, Cts. & Jud. Proc. § 10-401(4) ("information concerning the identity of the parties to the communication or the existence, substance, purport, or meaning of that communication"). The only difference between these definitions and those contained in the other wiretap statutes at issue in this case is the inclusion of "information concerning identity of the parties to the communication."

Though the definition differs slightly, the relevant analysis here remains the same under the Maryland and Massachusetts Acts as it does under the other statutes. As discussed more fully in Defendants' briefing on their motion to dismiss, the information that Plaintiffs allege was captured by the session replay technology included the users' mouse movements, clicks, keystrokes, and visited URLs, and this information does not convey the substance, purport, or meaning of a communication. (See ECF Nos. 54-1 at 11-14, 57 at 10). Nor do Plaintiffs adequately allege that this data is "information concerning the identity of the parties to the communication." While Plaintiffs make some allegations about how session replay software generally *could potentially* be configured to capture information regarding the identity of a website user (Compl. ¶¶ 75-80), they do not allege that BPS's software had the ability to capture identifying information, or that it actually did so, much less to Plaintiffs themselves.

Question 6 – As to the wiretap claims under the federal, California, and Maryland laws, provide your strongest authority as to whether Website Users allege a contemporaneous interception:

The authority cited in Defendants' motion to dismiss, along with Plaintiffs' own allegations, demonstrate that Plaintiffs have not alleged a contemporaneous interception under the federal, California, and Maryland laws. *See* ECF No. 54-1 at 14-15 (citing *Martin v. State*, 96 A.3d 765, 776 (Md. Ct. App. 2014) (Maryland Act); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir. 2002) (federal Act); *NovelPoster v. Javitch Canfield Grp.*, 140 F. Supp. 3d 938, 953 (N.D. Cal. 2014) (California Act)).

Each of these cases establishes that for an "interception" to be alleged under the respective statutes, the communication at issue must be intercepted "in transit." As the *NovelPoster* court explained, for modern electronic communications, "there is only a narrow window during which . . . an interception may occur—the seconds or mili-seconds before which a newly composed message is saved to any temporary location following a send command." 140 F. Supp. 3d at 951-52 (quoting *United States v. Steiger*, 318 F.3d 1039, 1050 (11th Cir. 2003).

Here, Plaintiffs' own allegations demonstrate that their communications—which they allege occurred between Plaintiffs on the one hand and Defendants' website on the other—were not intercepted in "the seconds or mili-seconds before which" they were "saved to any temporary location." To the contrary, Plaintiffs explicitly allege that Defendants' website "accumulate[s]" (in other words, saves) Plaintiffs' communications and then forwards those communications "in blocks periodically throughout the user's website session." Compl. ¶ 68.

Question 7 – As to the wiretap claims under the Maryland, Massachusetts, and Pennsylvania laws, provide your strongest authority as to whether session replay software is a "device":

As discussed more fully in Defendants' motion to dismiss, the Maryland, Massachusetts, and Pennsylvania statutes each limit themselves to communications that are captured by a "device." *See* ECF No. 54-1 at 15-18. Each of these states requires statutory language to be interpreted according to "common and approved usage." *See Commonwealth v. Hart*, 28 A.3d 898, 908 (Pa. 2011); *Schmerling v. Injured Workers' Ins. Fund*, 795 A.3d 715, 720 (Md. 2002); Mass. Gen. Laws. ch. 4 § 99(B)(3). As explained in Defendants' motion, the plain and ordinary meaning of a "device" is limited to something that is tangible. ECF no. 54-1 at 16-17 (citing Black's Law Dictionary (11th ed. 2019)).

While Defendants are not aware of any courts that have yet interpreted the Maryland, Massachusetts, or Pennsylvania laws so as to exclude session replay software from the statutory definition of "device," these principles of statutory interpretation, along with Plaintiffs' allegations that session replay code is merely "snippets of JavaScript computer code," mean that session replay code is not a "device" under the definition of the statutes.

As also noted in Defendants' motion to dismiss, other courts interpreting other, similar wiretap statutes have found session replay software to not be a "device." *See, e.g.*, *Jacome v. Spirit Airlines*, 2021 WL 3087860, at *6 (Fla. Cir. Ct. June 17, 2021); *Cardoso v. Whirlpool Corp.*, 2021 WL 2820822, at *2 (S.D. Fla. July 6, 2021); *Connor v. Whirlpool Corp.*, 2021 WL 3076477, at *2 (S.D. Fla. July 6, 2021). Notably, these courts uniformly found that session replay software was not a "device" under Florida's wiretap act despite Eleventh Circuit precedent suggesting that some other types of software—beyond the mere "snippets of JavaScript computer code" at issue for session replay—could qualify as a "device" under wiretap statutes. *See, e.g.*, *United States v. Barrington*, 648 F.3d 1178, 1203 (11th Cir. 2011) (assessing key logger software).

CONCLUSION

For these reasons, and those contained in Defendants' Motion and Reply Brief, Plaintiffs' Complaint should be dismissed in its entirety.

November 2, 2023

Respectfully Submitted,

By: */s/ Jennifer A. McLoone*

Erin (Loucks) Leffler (PA ID No. 204507)
Shook, Hardy & Bacon L.L.P.
Two Commerce Square
2001 Market St., Suite 3000
Philadelphia, PA 19103
Phone: (215) 278-2555
Fax: (215) 278-2594
eleffler@shb.com

Jennifer A. McLoone (admitted *pro hac vice*)
Shook, Hardy & Bacon L.L.P.
201 South Biscayne Boulevard
Suite 3200
Miami, FL 33131-4332
Phone: (305) 358-5171
Fax: (305) 358-7470
jmcloone@shb.com

Maveric Ray Searle (admitted *pro hac vice*)
Shook, Hardy & Bacon L.L.P.
111 South Wacker Drive
Suite 4700
Chicago, IL 60606
Phone: (312) 704-7741
Fax: (312) 558-1195
msearle@shb.com

Counsel for Defendants